Tugas Keamanan Jaringan Komputer

Case Hacking Ransomware WannaCry

Disusun Oleh:

Tamara Kharisma Restu (09011281419045)

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

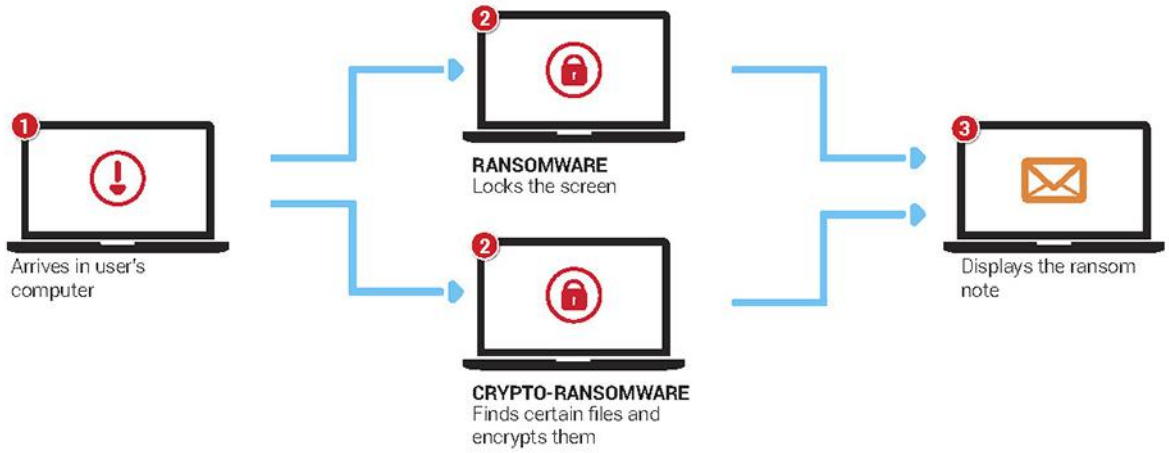
Ransomware WannaCry

Ransomware adalah malware yang mengacak data sehingga kita tidak dapat memakai komputer atau android. Pada Mei 2017, serangan siber skala besar menggunakan perangkat ini diluncurkan, menginfeksi lebih dari 75.000 komputer di 99 negara, menuntut pembayaran tebusan dalam 20 bahasa. Ransomware merupakan bentuk malware yang mengenkripsi dokumen pada PC atau bahkan di jaringan. Ransomware wanna cry kebanyakan menargetkan serangan ke industri kesehatan. Ransomware akan menghitung berapa kali setiap PC di-boot: setelah mencapai 90 kali dan mulai mengenkripsi mesin.

Awalnya, ransomware merupakan konstruksi yang relatif sederhana, dengan menggunakan kriptografi dasar yang sebagian besar hanya mengubah nama file, membuatnya relatif mudah untuk diatasi. Terutama dalam era transformasi digital sekarang ini, banyak perusahaan membangun aplikasi tanpa memperhatikan keamanan BYOD (*Bring Your Own Device*).

Salah satu varian yang paling sukses adalah 'Police ransomware', yang mencoba memeras korban dengan mengklaim sebagai penegak hukum dan mengunci layar dengan pesan memperingatkan pengguna bahwa mereka melakukan aktivitas online ilegal, yang bisa membuat mereka dikirim ke penjara.

Skenario WannaCry



1. Ransomware sering dimulai dengan email yang tidak di minta yang didesain untuk mengecoh pengguna untuk mengunjungi sebuah situs kemudian eminta protokol SMB (Server Message Block) untuk memindai port, lalu mencoba "DoublePulsar" backdoor untuk mengirim

WannaCry ke tujuan. Ransomware yang satu ini dibuat dengan menggunakan tool senjata siber dinas intel Amerika Serikat, NSA, yang dicuri dan dibocorkan grup hacker bernama Shadow Broker. Wanna Decryptor atau WannaCry atau wcry merupakan program ransomware spesifik yang akan mengunci semua data pada sistem komputer dan membiarkan pengguna hanya memiliki dua file, instruksi tentang apa yang harus dilakukan selanjutnya dan program Wanna Decryptor itu sendiri.

2. Saat software dibuka, komputer akan memberitahukan pengguna bahwa file mereka telah dienkripsi dan memberi waktu beberapa hari untuk membayar dengan memberi peringatan bahwa file akan dihapus.

3. WannaCry menginfeksi komputer lewat eksekusi remote code SMBv1 di sistem operasi Microsoft Windows. Sebelum dibocorkan oleh Shadow Broker, EnternalBlue sudah sering dipakai oleh NSA untuk mengendalikan komputer sasaran dari jarak jauh secara remote. Exploit ini bisa dipakai menyerang komputer yang menjalankan Windows XP hingga Windows Server 2012.

4. Begitu berhasil masuk ke sebuah komputer, WannaCry bisa menyebar dengan cepat ke komputer lain di lingkungan yang sama, misalnya di sebuah perusahaan. Seperti dijelaskan secara terpisah oleh firma keamanan Eset, WannaCry juga dibekali *worm* untuk memfasilitasi penyebarannya.

5. Ransomware mengenkripsi file pada sistem dan menuntut pambayaran uang tebusan dalam bitcoin (mata uang kripto) untuk merilisnya.

Cara Dasar dalam mencegah Ransomware WCry:

1. Lakukan backup secara berkala. Backup harus bersih dari infeksi ransomware.
2. Lakukan update selusuh sistem, firmware, dan sebagainya.
3. Lakukan monitoring secara pro-aktif seperti dengan menggunakan alat pengenalan pola perilaku data di jaringan dan storage.

4. Edukasi pengguna untuk tidak sembarang klik link URL dari website yang tidak jelas nama domainnya, dan juga tidak sembarang download lampiran di e-mail.

Dampak Ransomware WCry

Serangan tersebut mempengaruhi banyak rumah sakit Dinas Kesehatan di Inggris dan Skotlandia,dan sampai 70.000 perangkat termasuk komputer, pemindai MRI, lemari es penyimpanan darah.

Berbekal teknologi tool cyber NSA, WannaCry berhasil menyebar luas ke berbagai belahan dunia hanya dalam kurun waktu kurang dari dua hari sejak. Firma keamanan Avast mencatat bahwa *ransomware* ini telah menyerang puluhan ribu komputer di 99 negara di semua benua.

Di Inggris, 16 rumah sakit yang tergabung dalam jaringan National Health Service menjadi korban WannaCry. *Ransomware* itu mengganggu pelayanan kesehatan karena sistem-sistem komputer yang menyimpan rekam medis pasien jadi tidak bisa diakses.

Nissan Motor Manufacturing UK di Tyne and Wear, salah satu pabrik manufaktur mobil paling produktif di Eropa, menghentikan produksi setelah perangkat pemeras menginfeksi beberapa sistem mereka. Renault juga menghentikan produksi di beberapa lokasi dalam upaya menghentikan penyebaran perangkat pemeras tersebut.

Dampak serangan bisa jadi jauh lebih buruk jika tidak ada kill-switch yang dibangun oleh pencipta malware tersebut.